# 高度なフィッシング防御のためのOKTA SSO外部認証の設定

## 内容



## 概要

このドキュメントでは、Cisco Advanced Phishing Protectionへのログイン用にOKTA SSO外部認証を設定する方法について説明します。

## 前提条件

Cisco Advanced Phishing Protectionポータルへの管理者アクセス。

Okta idPへの管理者アクセス。

自己署名またはCA署名（オプション）PKCS #12またはPEM形式のX.509 SSL証明書。

## 背景情報

- Cisco Advanced Phishing Protectionを使用すると、SAMLを使用する管理者のSSOログインを有効にできます。
- OKTAは、アプリケーションに認証および許可サービスを提供するアイデンティティマネージャです。
- Cisco Advanced Phishing Protectionは、認証と認可のためにOKTAに接続するアプリケーションとして設定できます。
- SAMLは、XMLベースのオープン標準データ形式で、管理者がいずれかのアプリケーションにサインインした後、定義された一連のアプリケーションにシームレスにアクセスできるようにします。
- SAMLの詳細については、次のリンクにアクセスしてください。SAML一般情報

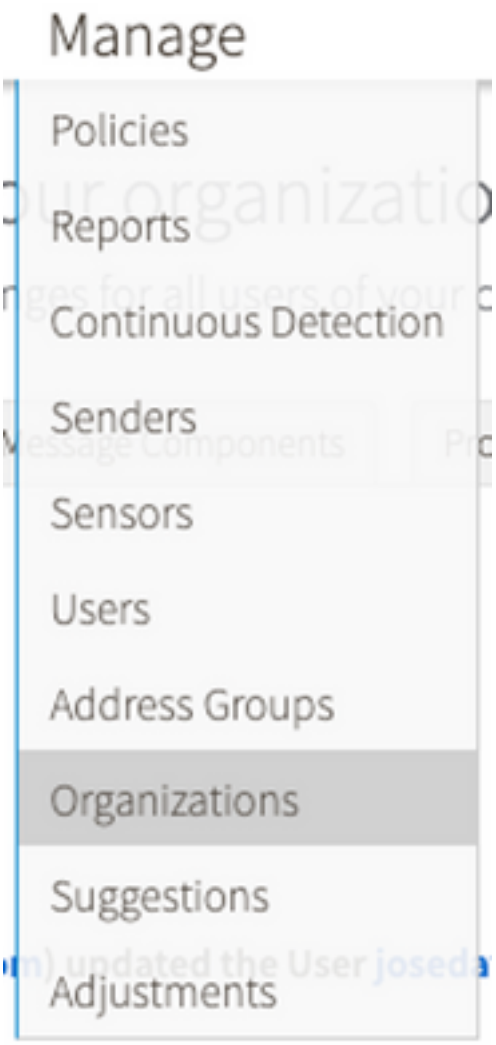
### 要件

- Cisco Advanced Phishing Protectionポータル。
- OKTA管理者アカウント。

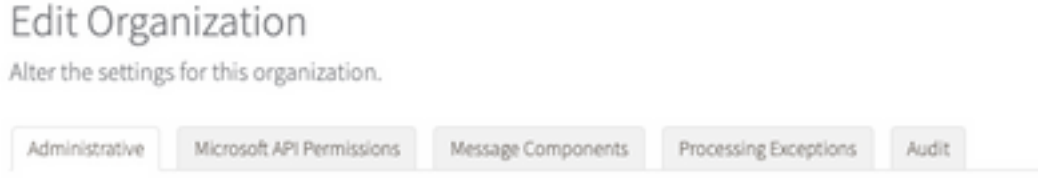
# 設定

**Cisco Advanced Phishing Protection Portalで、次の操作を実行します。**

1.組織ポータルにログインし、図に示すように[Manage] > [Organizations] を選択します。




2.次の図に示すように、組織名として[Edit Organization] を選択します。




3. [Administrative] タブで、[User Account Settings] まで下にスクロールし、図に示すように、[SSO]で[Enable] を選択します。


4.次のウィンドウに、OKTA SSO設定で入力する情報が表示されます。次の情報をメモ帳に貼り

付け、それを使用してOKTA設定を構成します。

– エンティティID:apcc.cisco.com

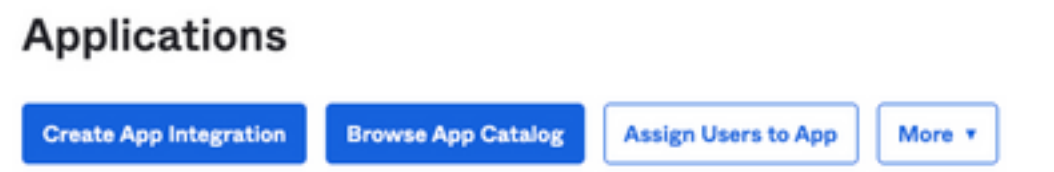
– アサーションコンシューマサービス：このデータは組織に合わせてカスタマイズされます。

次の図に示すように、ログインに電子メールアドレスを使用する名前付き形式**e-mail**を選択します。

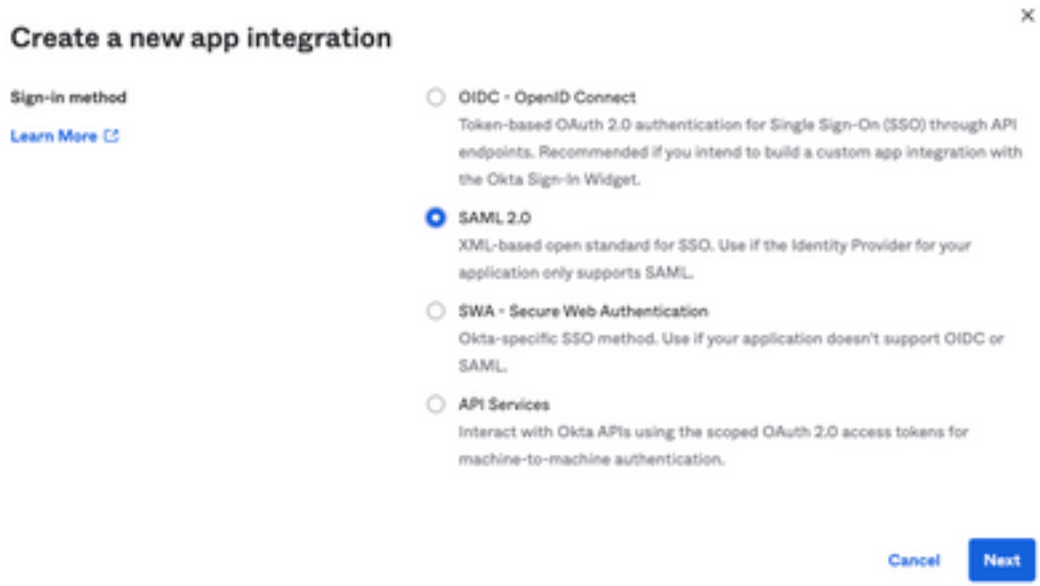

5.次の手順に進む前に、まずOKTAでアプリケーションを設定する必要があるため、現時点ではCisco Advanced Phishing Protectionの設定を最小化します。

**オクタの下で。**

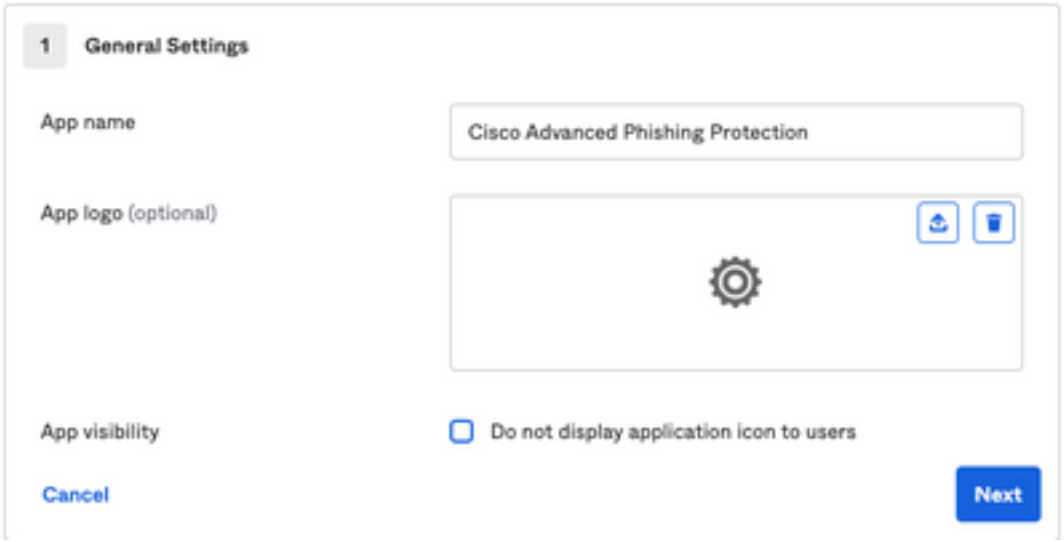
1. [Applications]ポータルに移動し、図に示すように[Create App Integration] を選択します。




2.図に示すように、アプリケーションタイプとして**SAML 2.0**を選択します。




3.次の図に示すように、アプリケーション名**Advanced Phishing Protection**を入力し、[Next] を選択します。




4. SAML設定で、図に示すようにギャップを入力します。

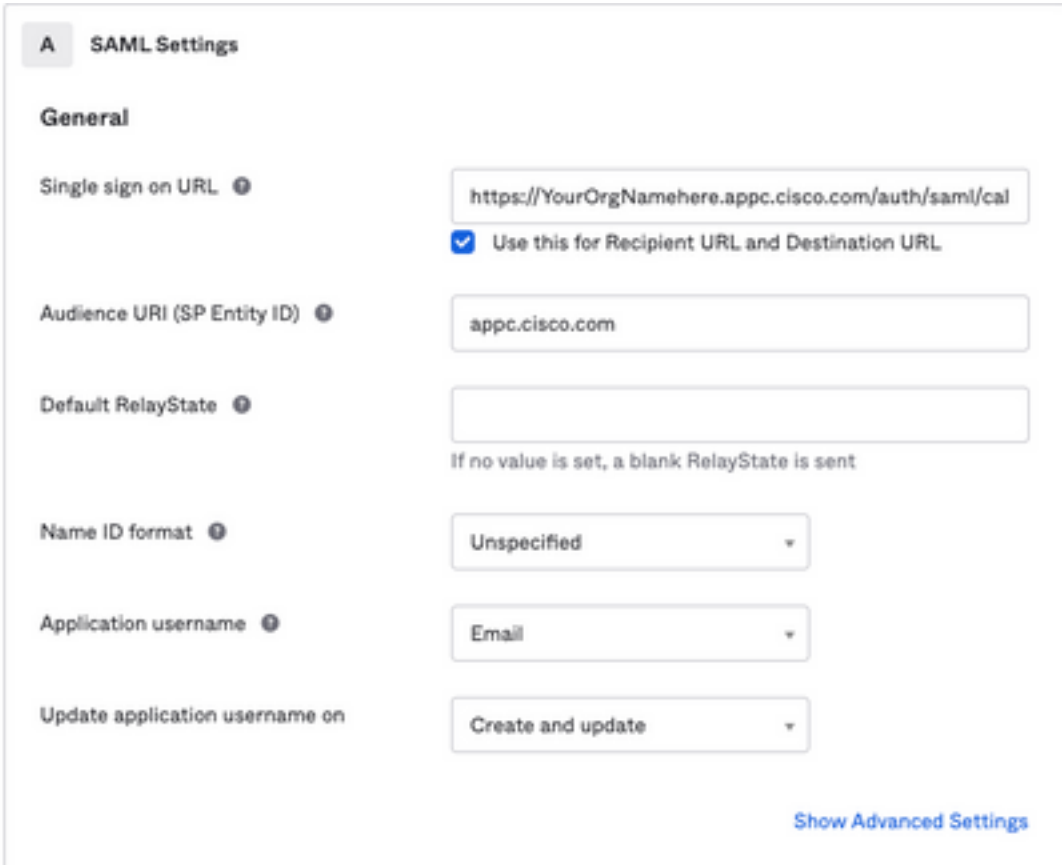
– シングルサインオンURL:これは、Cisco Advanced Phishing Protectionから取得したアサーションコンシューマサービスです。

– 受信者URL:これは、Cisco Advanced Phishing Protectionから取得したエンティティIDです。

– 名前IDの形式：未指定のままにしておきます。

– アプリケーションユーザ名：電子メール：認証プロセスで電子メールアドレスの入力をユーザに求めます。

– アプリケーションのユーザー名の更新日時：作成および更新




図に示すように、[Group Attribute Statements (optional)] まで下にスクロールします。

次の属性文を入力します。

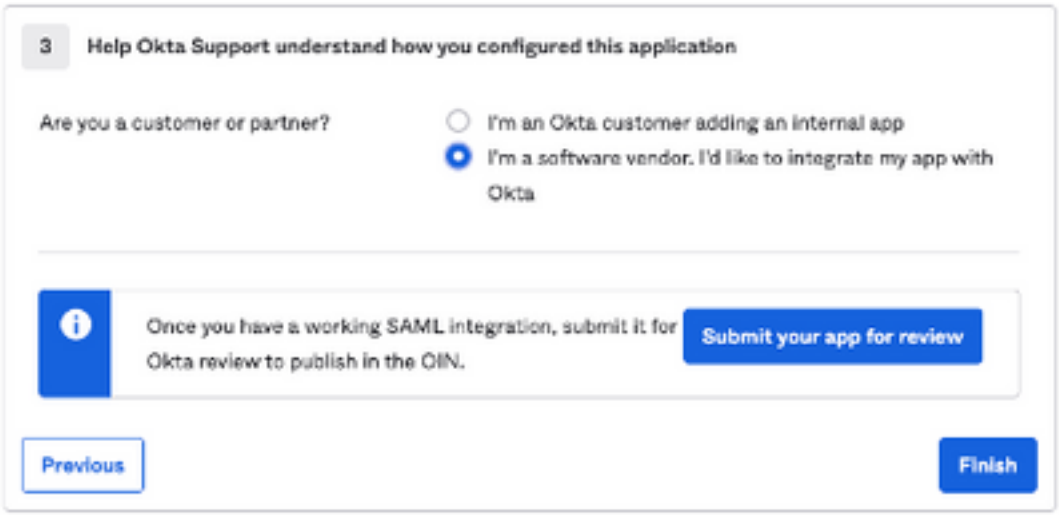
-Name：グループ

– 名前の形式：未指定。

-フィルタ:「Equals」および「OKTA」

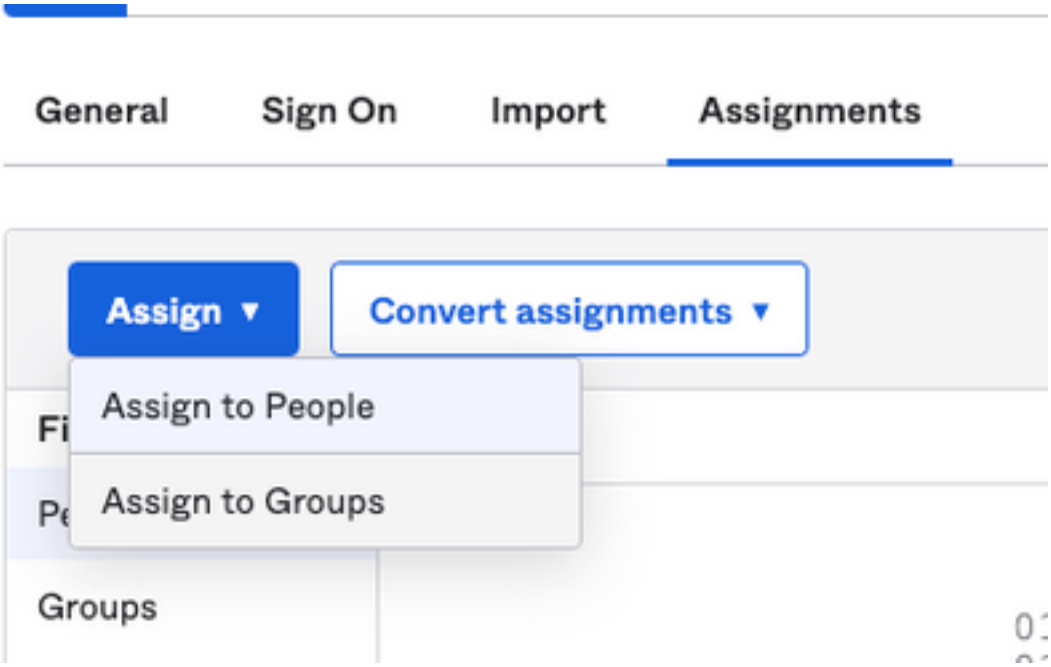

[次へ（Next）] を選択します。

5.このアプリケーションの設定方法をHelp Oktaに尋ねられたら、図に示すように、現在の環境に該当する理由を入力してください。



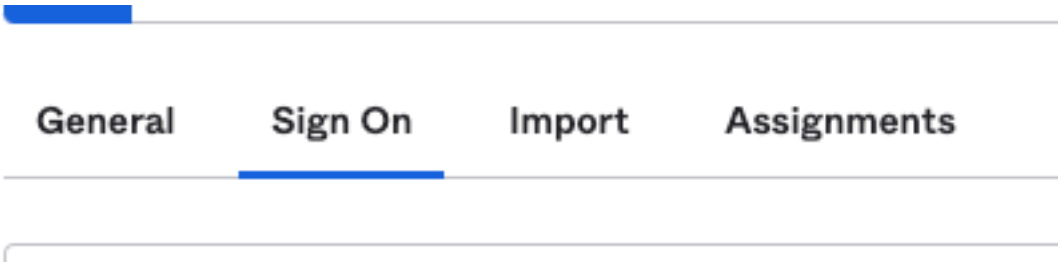

**Finish**を選択して、次のステップに進みます。

6. [Assignments] タブを選択し、次の図に示すように[Assign] > [Assign to Groups] を選択します。

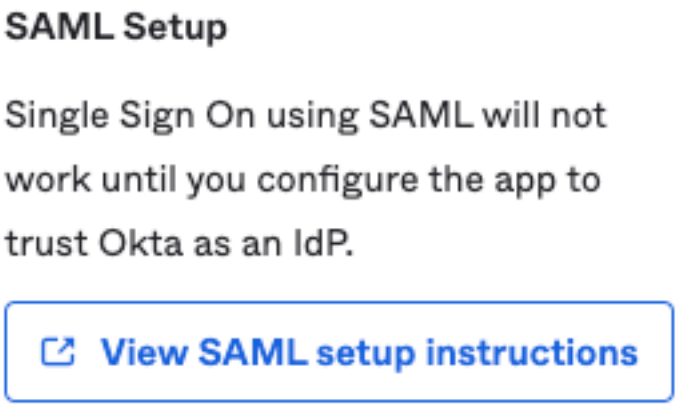



7. OKTAグループを選択します。このグループは、環境にアクセスする権限を持つユーザーのグループです

8.図に示すように、[Sign On] を選択します。




9.図に示すように、下にスクロールして右隅に移動し、[View SAML setup instructions] オプションを入力します。

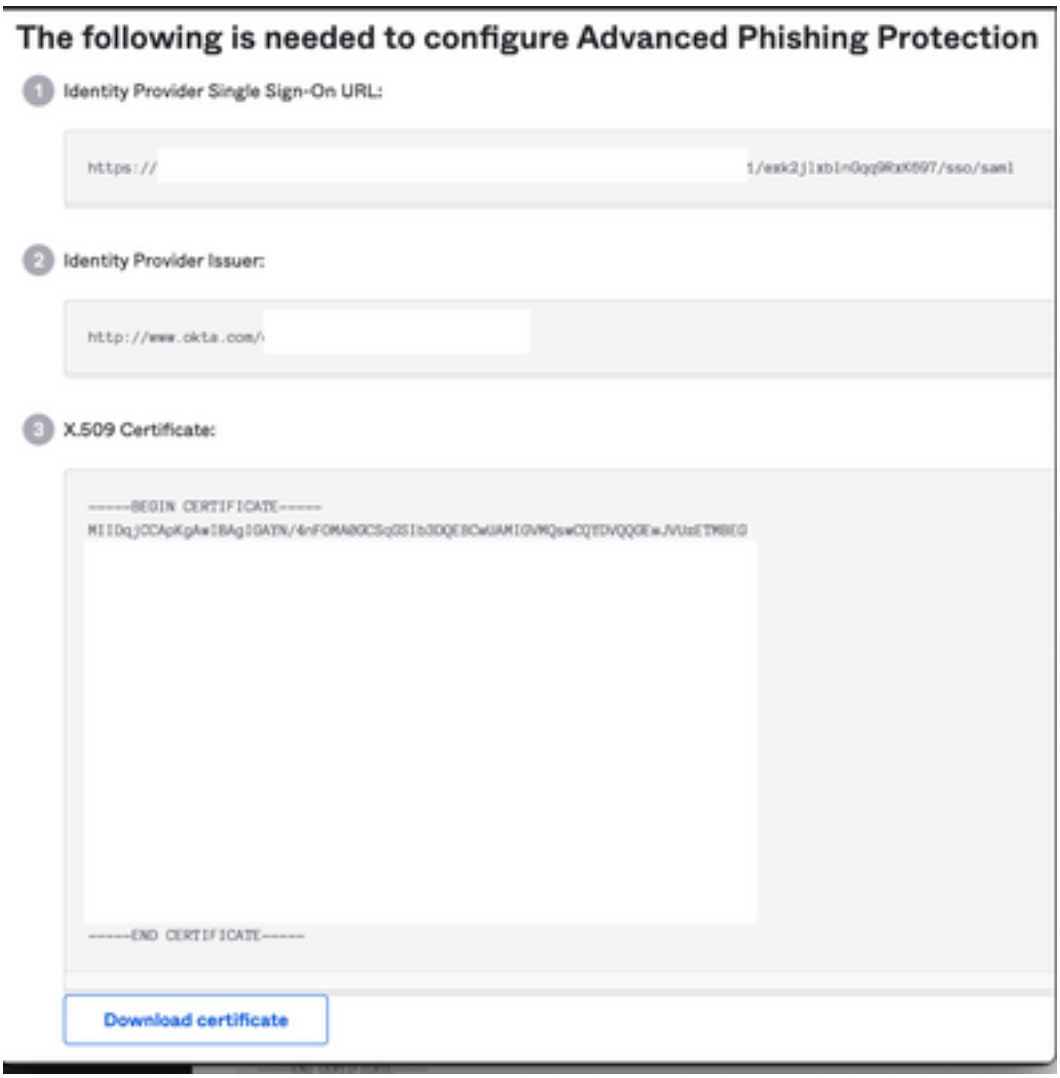



9.次の図に示すように、次の情報をメモ帳に保存します。この情報は、Cisco Advanced Phishing Protectionポータルに追加するために必要です。

– アイデンティティプロバイダーのシングルサインオンURL。

– プロバイダー発行者を特定します(Cisco Advanced Phishing Protection(AFP)には必要ありませんが、他のアプリケーションには必須です)。

- X.509証明書。




10. OKTAの設定が完了したら、Cisco Advanced Phishing Protectionに戻ることができます

**Cisco Advanced Phishing Protection Portalで、次の操作を実行します。**

1.「名前識別子フォーマット」で、次の情報を入力します。

- SAML 2.0エンドポイント（HTTPリダイレクト）:Oktaから提供されたIdentify Provider Single Sign-On URL。

– 公開証明書：Oktaから提供されたX.509証明書を入力します。

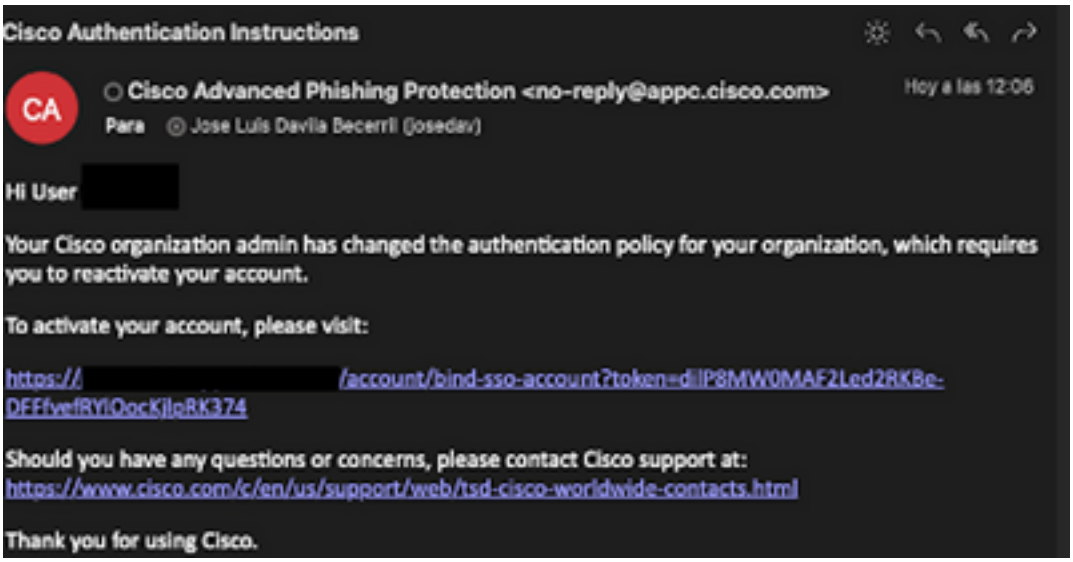
2. [Test Settings] を選択して、設定が正しいことを確認します

設定にエラーがない場合は、[Test Successful]エントリが表示され、図に示すように設定を保存できます。

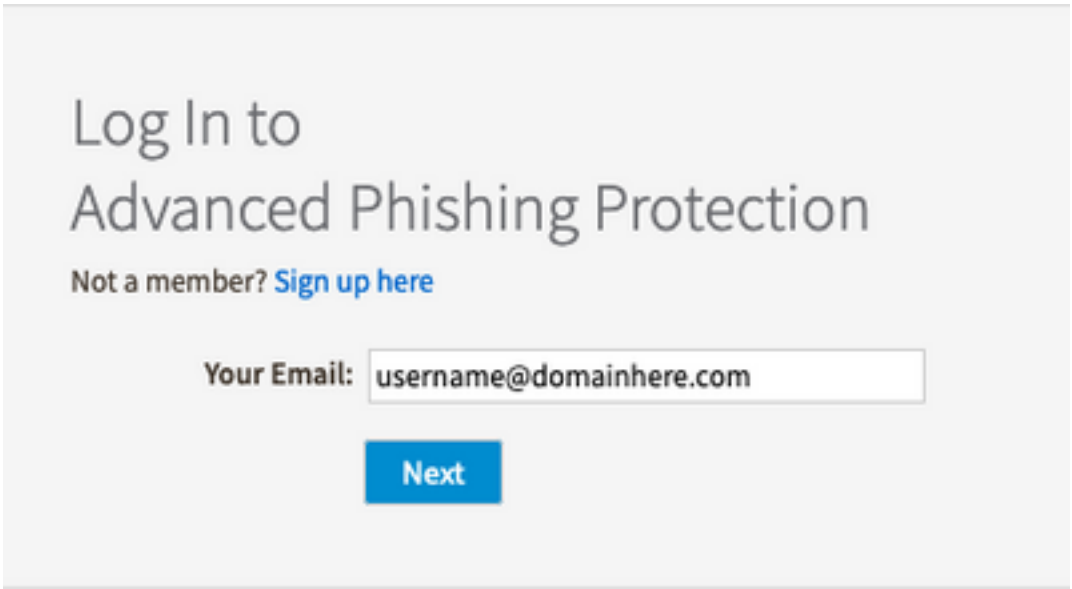
3.設定の保存

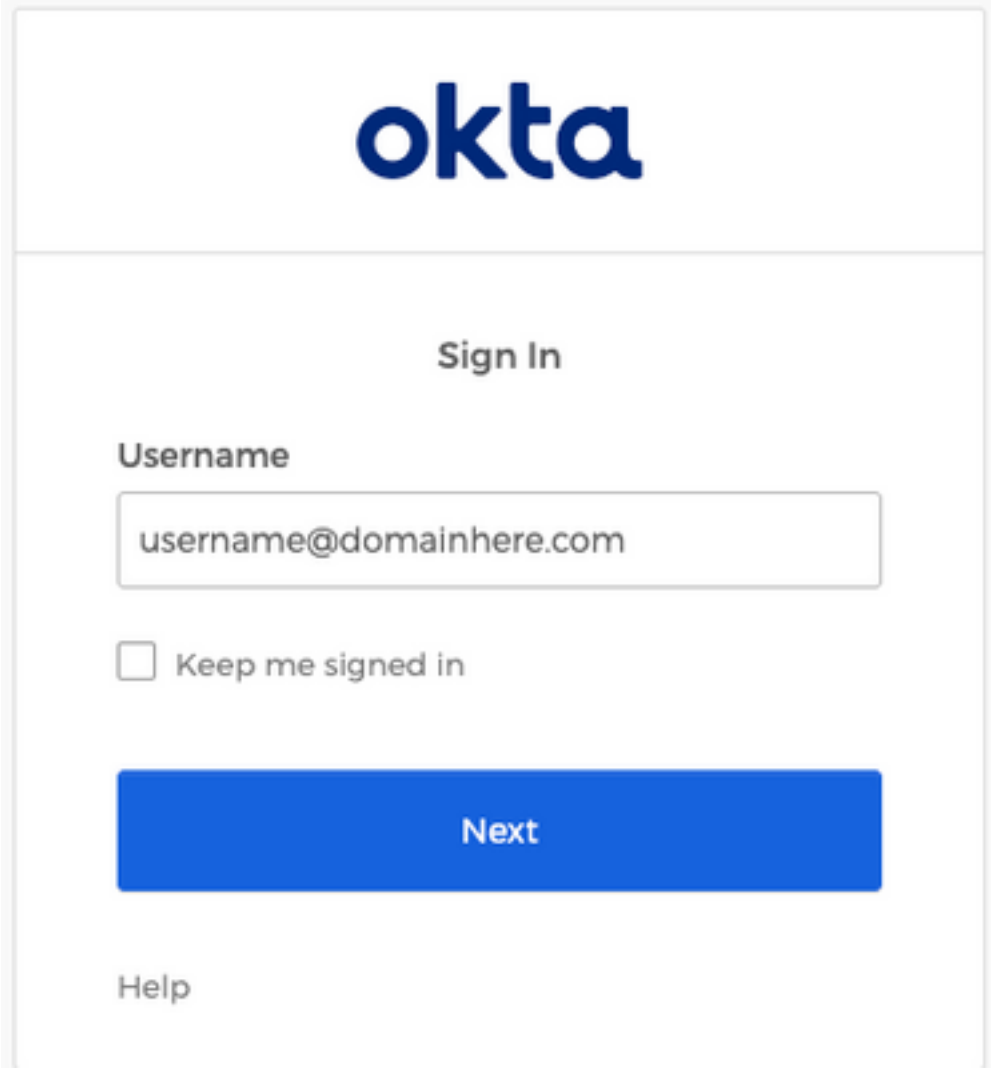
## 確認

1. SSOを使用していない既存の管理者は、次の図に示すように、組織の認証ポリシーが変更されたことを電子メールで通知され、管理者は外部リンクを使用してアカウントをアクティブにするように求められます。

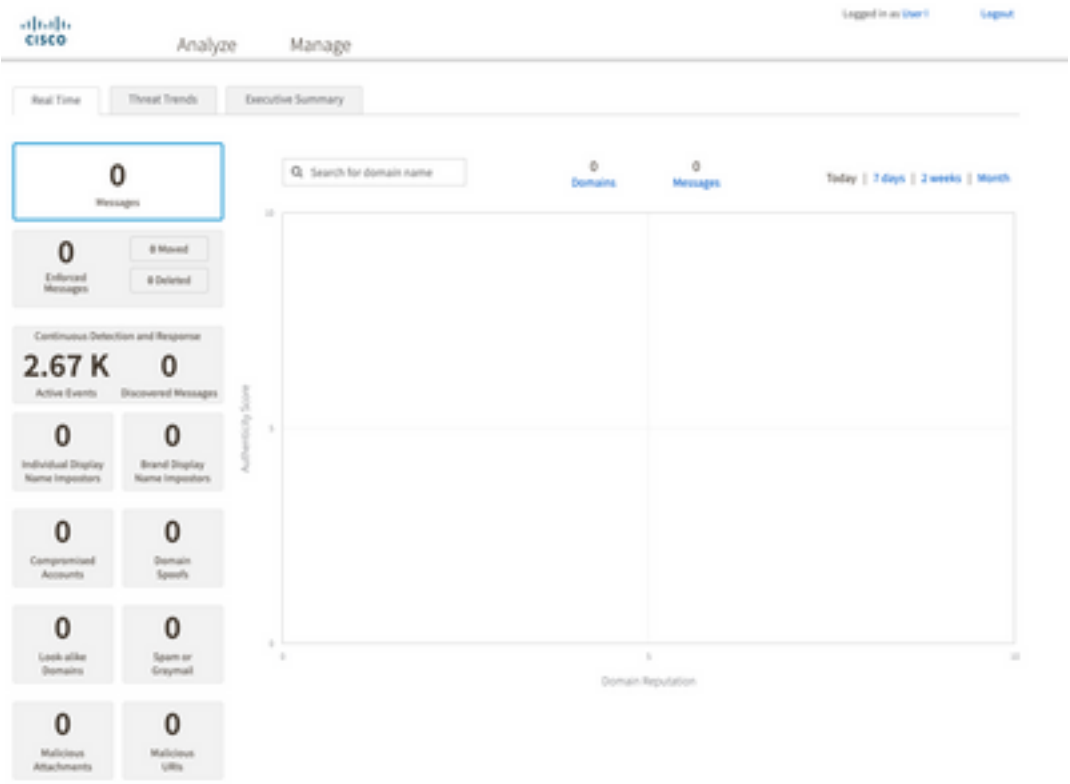



2.アカウントがアクティブになったら、次の図に示すように、電子メールアドレスを入力し、OKTAログインWebサイトにリダイレクトしてログインします。






3. OKTAログインプロセスが完了したら、図に示すように、Cisco Advanced Phishing Protectionポータルにログインします。



# 関連情報

Cisco Advanced Phishing Protection – 製品情報

Cisco Advanced Phishing Protection – エンドユーザガイド

OKTAサポート

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。